A METHOD FOR GENERATING ASYMMETRICAL CRYPTOKEYS AT THE USER'S LOCATION

Background Information

The present invention relates to an asymmetrical cryptological method ~~of the type described in more detail in the preamble of patent Claim 1. Methods of this type are widely known and are described, e.g., in~~ Menezes: Handbook of Applied Cryptography, 1997.

A crucial problem of all known open cryptological methods is the reliable assignment to the authorized user of the utilized signature and encryption keys and the confirmation of the assignment by an independent third entity. In technical terms, this is a question of the reliable personalization of the keys along with subsequent certification.

Trustworthy methods, such as are described by Kowalski, in The Telecommunications Engineer 4/5 1995: "Security Management System," solve this problem currently by generating, personalizing, and certifying keys of this type at a central, particularly secure location (usually so-called Trust Centers).

However, it cannot be excluded that in the future the users themselves will increasingly wish to generate their cryptokeys, in particular those for encryption. This desire should not be realized at the expense of the security and reliability of the method in question, as is the case today in the only loosely organized asymmetrical cryptological methods of the Internet.

Summary of the Invention

Thus as the objective of the invention, a method is required which shifts the generation of keys into the area of responsibility of the user without forfeiting the organizational security of an independent entity.

~~This objective is achieved in the method indicated in the characterizing part of Patent Claim 1~~.

Advantageous possibilities for refinements are apparent in the characterizing part of Subclaim 2.

Detailed Description

The invention is explained on the basis of the following exemplary embodiment:

The user receives from the central location, hereinafter termed Trust Center, a signature key pair that is already generated, personalized, and certified, e.g., a private signature key PS and a public signature key ÖS as well as the components for producing one or more encryption key pairs, Generate Encryption Keys, GEK.

The user then himself produces at any time an encryption key pair, e.g., a private encryption key PVS, marks the public part of this pair, public encryption key OVS, using the previously relinquished secret signature key PS, and transmits the result to the Trust Center. There, using a check with the aid of the certified public part of the signature key pair ÖS of the user, the result is to be assigned as belonging, unequivocally and reliably, to the user.

The Trust Center thereupon generates a new certificate, in which are contained either both the public part of signature key pair ÖS as well as that of encryption key pair ÖVS, or only that of the encryption key pair ÖVS of the user.

This certificate, in the next step, is then encrypted using the public part of the encryption key pair ÖVS of the user and is then transmitted.

Thus it is assured that only the authorized user is able to decode the certificate and, in hardware-based systems, can download it into his corresponding hardware. At no time does the user have to reveal his secret, namely the secret part of encryption key pair PVS.

If the user also wishes to generate the signature key pair in his area of responsibility, in other words if he also wants to protect the secret part of a signature key pair, a second private signature key PS2, from being accessed by the Trust Center, then this method is also used analogously for this purpose. Only the components Generate Digital Signature Keys, GDSK, for producing one or

more signature key pairs, are also relinquished to the user.

Once generated, with the aid of the secret signature key PS relinquished by the Trust Center, the user also marks the public part of self-generated signature key pair ÖS2, in addition to or simultaneous with the public part of self-generated encryption pair ÖVS, and the result is transmitted to the Trust Center, where subsequently the process is continued just as described above.

If user AW1 does not wish to have any further communication with a Trust Center, he can do this as well using the described method without any loss of reliability, by first marking and making available to the communication partner the public part of his self-generated key pair ÖVS using the secret part of the previously relinquished, personalized, and certified key pair PS in every bilateral communication with another user AW2.

Receiving communication partner AW2 can reliably check the correct assignment of this information with regard to public part ÖVS of the key pair self-generated by sending user AW1 by verifying the signature and, if necessary, checking the genuineness and validity of the certificate in the Trust Center underlying this signature.